UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/752,420	01/05/2004	Gregory Gordon Rose	030010	3858

23696 7590 07/03/2008
QUALCOMM INCORPORATED
5775 MOREHOUSE DR.
SAN DIEGO, CA 92121

EXAMINER	
KANE, CORDELIA P	

ART UNIT	PAPER NUMBER
2132	

NOTIFICATION DATE	DELIVERY MODE
07/03/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

us-docketing@qualcomm.com
kascanla@qualcomm.com
nanm@qualcomm.com

Office Action Summary	**Application No.** 10/752,420	**Applicant(s)** ROSE ET AL.	
	Examiner CORDELIA KANE	**Art Unit** 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 April 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-51* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-51* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on April 23, 2008 has been entered.

Response to Arguments

2. Applicant's arguments with regards to the combination of references filed April 23, 2008 have been fully considered but they are not persuasive. In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992).

3. In the case of Hollis and Schneier, it would have been obvious to combine Hollis with Schneier because it is a more secure way to protect a backup key (page 182, 2nd paragraph).

4. In the case of Hollis in view of O'Shea it would have been obvious to combine Hollis in view of O'Shea because the heavy cost of authentication may impeded the growth of mobile networks and without suitable authentication mechanism that new wireless networks are vulnerable to simple attacks (page 1, paragraph 6).

Claim Rejections - 35 USC § 112

5. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

6. Claims 10 and 15 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventors, at the time the application was filed, had possession of the claimed invention. There is no mention in the specification of preventing retransmission of the second private key.

7. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

8. Claim 7 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 7 states that the second public and private keys are created independently from the first public and private keys, however it is specifically

stated in claim 1 that the second private key is associated with the first private key. It is not possible for the two to be independent when earlier they are defined as being associated.

Claim Rejections - 35 USC § 101

9. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

10. Claims 14 - 21,and 40 - 42 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. In the specification applicant defines the means to include software only [0064].

Claim Rejections - 35 USC § 103

11. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

12. Claims 1, 11 – 14, 19 – 22, 26 – 28, 50 and 51 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hollis, and further in view of O’Shea. Referring to claims 1, 14 and 22, Hollis teaches:

a. Creating a first and second private and public key pair (column 24, lines 39-40).

b. Both the second public and private key are outputted (column 24, line 41).

c. The second public key and the first public key being outputted concurrently (column 24, lines 5-7). While the second public key is described as an offline backup earlier in the specification it is defined that both keys are distributed.

d. It is inherent that the first private key would be used for authentication since it is not the backup. Also, it is specifically stated that it is used for authentication (column 8, lines 59-60).

13. Hollis fails to teach creating the keys at a mobile device, wirelessly transmitting the keys, and then authenticating at the mobile device. However, O'Shea teaches that the sender is a mobile device (abstract) and the sender holding the public-private key pair (page 2, paragraph 9), which is then used to authenticate the sender using the public-private key pair (page 1, paragraph 8). Also, O'Shea teaches that the mobile device communicates via wireless (page 3, paragraph 25).

14. Hollis and O'Shea are analogous art because they are from the same field of endeavor, encryption. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Hollis and O'Shea before him or her, to modify the key system of Hollis to include the mobile devices of O'Shea. The suggestion/motivation for doing so would have been that the heavy cost may impeded the growth of mobile networks and without suitable authentication mechanism that new wireless networks are vulnerable to simple attacks (page 1, paragraph 6).

15. Referring to claims 11, 19, and 26, Hollis discloses:

e. Receiving a first public key (column 9, lines 63-64).

f. Receiving a second public key, the second public key and the first public key being outputted concurrently (column 24, lines 5-7). While the second public key is described as an offline backup earlier in the specification it is defined that both keys are distributed.

g. Using the first public key for authentication (column 14, lines 38-40, column 8, lines 59-60).

h. Using the second public key for authentication if the first public key fails (column 10, lines 31-36).

16. Hollis does not explicitly disclose receiving the public keys from the mobile user device, wirelessly transmitting the keys, and authenticating the mobile user device. However, O'Shea discloses outputting the public key (page 2, paragraph 9), and then authenticating using the public-private key pair (page 1, paragraph 8). Also, O'Shea teaches that the mobile device communicates via wireless (page 3, paragraph 25).

17. Hollis and O'Shea are analogous art because they are from the same field of endeavor, encryption keys. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Hollis and O'Shea before him or her, to modify the key system of Hollis to include the mobile devices of O'Shea. The suggestion/motivation for doing so would have been that the heavy cost may impeded the growth of mobile networks and without suitable authentication mechanism that new wireless networks are vulnerable to simple attacks (page 1, paragraph 6).

18. Referring to claims 12, 20 and 27, Hollis teaches the creation of a primary key and a backup key (column 24, lines 39-41). It would have been obvious to modify Hollis to create a third private and public key pair, once the backup (second) key had been used, as taught by Hollis (column 10, line 23), since there would need to be a new

backup. It would have been obvious that after creation of the new backup key pair to distribute the new (third) public key since it would be needed for future authentication.

19. Referring to claims 13, 21, and 28, Hollis teaches the creation of a primary key and a backup key (column 24, lines 39-41). It would have been obvious to modify Hollis to create a third private and public key pair, once the backup key had been used since there would need to be a new backup. It would also be obvious to repeat that process again and create a fourth backup pair of keys. It would have been obvious to then distribute the third and fourth public keys since they would be needed for future authentication.

20. Referring to claim 50, Hollis teaches:

i. A processor for creating a first and second private and public key pair (column 24, lines 39-40).

j. A storage medium to store the first private key (column 9, line 55).

k. A transmitter to output the second private and public key pair (column 24, line 41) at the same time as the first public key (column 24, lines 43-44).

l. Using the first private key for authenticating is inherent from the fact that it is not the backup.

21. Hollis fails to teach wirelessly transmitting the keys, and then authenticating at the mobile device. However, O'Shea teaches that the sender is a mobile device (abstract) and the sender holding the public-private key pair (page 2, paragraph 9), which is then used to authenticate the sender using the public-private key pair (page 1,

paragraph 8). Also, O'Shea teaches that the mobile device communicates via wireless (page 3, paragraph 25).

22. Hollis and O'Shea are analogous art because they are from the same field of endeavor, encryption. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Hollis and O'Shea before him or her, to modify the key system of Hollis to include the mobile devices of O'Shea. The suggestion/motivation for doing so would have been that the heavy cost may impeded the growth of mobile networks and without suitable authentication mechanism that new wireless networks are vulnerable to simple attacks (page 1, paragraph 6).

23. Referring to claim 51, Hollis teaches:

m. Receiving a first public key (column 9, lines 64-65) and a second public key (column 10, lines 33-34).

n. A storage medium for storing both the first and second public keys (column 9, lines 59-61).

o. A processor that knows to use the second public key when the first key fails (column 10, lines 35-36). Using the first public key for authentication is inherent from it not being the backup key.

24. Hollis does not explicitly disclose receiving the public keys from the mobile user device, wirelessly transmitting the keys and using the public keys for authentication of the mobile user device. However, O'Shea discloses outputting the public key (page 2, paragraph 9), and then authenticating using the public-private key pair (page 1,

paragraph 8). Also, O'Shea teaches that the mobile device communicates via wireless (page 3, paragraph 25).

25. Hollis and O'Shea are analogous art because they are from the same field of endeavor, encryption keys. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Hollis and O'Shea before him or her, to modify the key system of Hollis to include the mobile devices of O'Shea. The suggestion/motivation for doing so would have been that the heavy cost may impeded the growth of mobile networks and without suitable authentication mechanism that new wireless networks are vulnerable to simple attacks (page 1, paragraph 6).

26. Claims 2 – 6, 8 - 10, 15 – 18, and 23 – 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hollis in view of O'Shea and further in view of Bruce Schneier's Applied Cryptography. Referring to claims 2, 15 and 23, Hollis in view of O'Shea teaches all the limitations of the parent claims, but fails to teach the splitting of the second public key into shares. Schneier goes on to teach that it is the best method to split the key into pieces and share the key between different entities (page 182, 1st and 2nd paragraph). It would have been obvious to modify Hollis in view of O'Shea to separate the backup key into different parts and distribute to different entities, as taught by Schneier, because it is more secure, since the key is protected against malicious attacks (page 182, paragraph 2).

27. Referring to claims 3, 16 and 24, Hollis in view of O'Shea teaches using the second private key for authentication (Hollis, column 10, line 23). Hollis in view of

O'Shea fails to teach the recreation of the second private key. Schneier teaches that separating the keys is a better way to secure backup keys and that when it comes time to use them that you have to reconstruct them (page 182 2nd paragraph). It would have been obvious to modify Hollis in view of O'Shea to reconstruct the keys, as taught by Schneier, because it is a more secure way to store the backup key since it will protect it against malicious attacks (page 182, 2nd paragraph).

28. Referring to claims 4 and 25, Hollis teaches disabling the first private key when the second is used for authentication (Hollis, column 14, lines 46-48). O'Shea discloses that the public private key pair is used for the authentication (O'Shea, page 1, paragraph 8).

29. Referring to claims 5 and 17, Hollis in view of O'Shea teaches the creation of a primary key and a backup key (Hollis, column 24, lines 39-41). It would have been obvious to modify Hollis to create a third private and public key pair, once the backup key had been used since there would need to be a new backup. It also would have been obvious to then distribute the new backup public key. Hollis does not disclose that the key is outputted from the mobile user device. However, O'Shea teaches that the mobile device outputs the public key (page 2, paragraph 9).

30. Referring to claim 6, Hollis in view of O'Shea teaches using the third private key for authentication (Hollis, column 10, line 23), and holding the private key at the user device (O'Shea, page 1, paragraph 9). Hollis in view of O'Shea fails to teach the outputting of the third key in separate pieces. Schneier teaches that it is a more secure method with backup keys (third key) to split it into separate parts and distribute them to

different entities, which is the same as outputting it so that it can be recreated. Schneier goes on to teach how then the pieces can then be brought back together to be recreated (page 182, second paragraph). It would have been obvious to modify Hollis in view of O'Shea to split the key into separate pieces since it is a more secure method for backup keys.

31. Referring to claims 8 and 18, Hollis in view of O'Shea teaches the creation of a primary key and a backup key (Hollis, column 24, lines 39-41). It would have been obvious to modify Hollis in view of O'Shea to create a third private and public key pair, once the backup key had been used since there would need to be a new backup. It would also be obvious to repeat that process again and create a fourth backup pair of keys. It would then be inherent to distribute both new public keys. Schneier teaches distributing pieces of a private key to be used for recreation later (page 182, second paragraph). Since the fourth key pair would now be the backup, it would have been obvious to modify Hollis in view of O'Shea so that it distributes pieces of the fourth private key for recreation later since it is a more secure way to store backups.

32. Referring to claim 9, Hollis in view of O'Shea teaches using a new (third) private key for authentication (Hollis, column 10, line 23). Hollis in view of O'Shea goes on to teach the disabling of the old (second) key for authentication (Hollis, column 14, lines 46-48). Hollis teaches using a new (fourth) private key for authentication (column 10, line 23). It fails to teach the recreation of the fourth private key. Schneier teaches that separating the keys is a better way to secure backup keys and that when it comes time to use them that you have to reconstruct them (page 182 second paragraph). It would

have been obvious to modify Hollis in view of O'Shea to reconstruct the keys, as taught by Schneier, because it is a more secure way to store the backup key.

Referring to claim 10, Hollis in view of O'Shea teaches preventing retransmission of the second private key (Hollis, column 14, lines 46-48).

33. Claims 29, 30, 33, 34, 36, 37, 40, 41, 43, 44, 47 and 48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schwenk, and further in view of O'Shea.

Referring to claims 29 and 43, Schwenk teaches:

p. Creating a private (v) and public key (V) using a system parameter (g) (column 4, line 43)

q. Outputting the public key and the system parameter (column 4, lines 43-45). While it is not specifically stated that g is outputted, both entities have it so it can be inferred that it was outputted.

r. The private key v is used to create the public key V, therefor it is used for authentication. The authentication of the recipient takes place when the private key is used to decrypt the message (column 1, lines 40-41). This way the recipient knows it was the intended recipient of the message.

34. Schwenk fails to teach creating the keys at a mobile device, wirelessly transmitting the keys, and then authenticating at the mobile device. However, O'Shea teaches that the sender is a mobile device (abstract) and the sender holding the public-private key pair (page 2, paragraph 9), which is then used to authenticate the sender

using the public-private key pair (page 1, paragraph 8). Also, O'Shea teaches that the mobile device communicates via wireless (page 3, paragraph 25).

35. Schwenk and O'Shea are analogous art because they are from the same field of endeavor, encryption keys. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Schwenk and O'Shea before him or her, to modify key regeneration system of Schwenk to be on the mobile device of O'Shea. The suggestion/motivation for doing so would have been to be able to reconstruct the key in the event it is lost (Schwenk, column 5, line 55).

36. Referring to claims 30 and 44, Schwenk teaches:

s. Creating a new private key C using the previous private key v and the system parameter (column 4, lines 56-59). The system parameter g is used to calculate R and therefor S, which is then used to calculate C.

t. The secret key is used for authentication (column 4, line 53-54).

37. Referring to claims 33, 40 and 47, Schwenk discloses:

u. Receiving a public key V, and a system parameter g (column 4, lines 43-45).

v. Generating a new public key U using the seed value S after the loss of a key (column 3, lines 59-61). The seed value S is derived from the system parameter g and the public key V, therefor the public key and system parameter are used to generate the new public key. It is inherent that the public key would have failed otherwise the system would not know that the key had been lost (column 4, line 55).

38. Schwenk fails to teach the keys being received at the mobile device, or wirelessly transmitting the data. However, O'Shea discloses the mobile device outputting the public key (page 2, paragraph 9). Also, O'Shea teaches that the mobile device communicates via wireless (page 3, paragraph 25). Schwenk and O'Shea are analogous art because they are from the same field of endeavor, encryption keys. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Schwenk and O'Shea before him or her, to modify key regeneration system of Schwenk to be on the mobile device of O'Shea. The suggestion/motivation for doing so would have been to be able to reconstruct the key in the event it is lost (Schwenk, column 5, line 55).

39. Referring to claims 34, 41 and 48,, Schwenk teaches generating a new public key U using the seed value S (column 2, lines 59-63) which is derived using powers of the previous public key V (Figure 1). It is inherent that the public key that works would be accepted.

40. Referring to claim 36, Schwenk teaches:

w. Creating a private (v) and public key (V) using a system parameter (g) (column 4, line 43)

x. Outputting the public key and the system parameter (column 4, lines 43-45). While it is not specifically stated that g is outputted, both entities have it so it can be inferred that it was outputted.

41. Schwenk does not explicitly disclose using the private key for authentication of the mobile user device. However, O'Shea discloses that the private key is used for

authentication of the mobile device (page 1, paragraph 8). Schwenk and O'Shea are analogous art because they are from the same field of endeavor, encryption keys. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Schwenk and O'Shea before him or her, to modify key regeneration system of Schwenk to be on the mobile device of O'Shea. The suggestion/motivation for doing so would have been so the recipient can authenticate the information based only on the data provided (page 1, paragraph 8).

42. Referring to claim 37, Schwenk teaches creating a new private key C using the previous private key v and the system parameter (column 4, lines 56-59). The system parameter g is used to calculate R and therefor S, which is then used to calculate C.

43. Claims 31, 32, 35, 38, 39, 42, 45, 46, and 49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schwenk in view of O'Shea and further in view of Liao. Referring to claims 31 and 45, Schwenk in view of O'Shea teaches the limitations of the parent claim. It fails to teach the use of a counter value. Liao teaches the use of a counter value to keep track of the generations of key regeneration (column 15, line 59-61). It would have been obvious to modify Schwenk in view of O'Shea to include a counter value, as taught by Liao, because it would be more efficient to keep track of how many iterations have been through (column 15, lines 59-61).

44. Referring claims 32 and 46, Schwenk teaches:

y. Creating a new private key C using the previous private key v and the system parameter (column 4, lines 56-59). The system parameter g is used to calculate R and therefor S, which is then used to calculate C.

z. The secret key is used for authentication (column 4, line 53-54).

45. Schwenk in view of O'Shea fails to teach using a counter in the calculation. Liao teaches the use of a counter value to keep track of the generations of key regeneration (column 15, line 59-61). It would have been obvious to modify Schwenk to include a counter value, as taught by Liao, because it would be more efficient to keep track of how many iterations have been through (column 15, lines 59-61).

46. Referring to claims 35, 38, 42 and 49, Schwenk in view of O'Shea discloses all the limitations of the parent claim. Schwenk in view of O'Shea does not explicitly disclose receiving a counter value. However, Liao teaches the use of a counter value to keep track of the generations of key regeneration (column 15, line 59-61). Schwenk in view of O'Shea and Liao are analogous art because they are from the same field of endeavor, encryption keys. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Schwenk in view of O'Shea and Liao before him or her, to modify the key regeneration system in a mobile device of Schwenk in view of O'Shea to include the counter values of Liao. The suggestion/motivation for doing so would have been to keep track of the amount of key regenerations (column 15, lines 59-61).

47. Referring to claim 39, Schwenk in view of O'Shea discloses all the limitations of the parent claims. Schwenk in view of O'Shea fails to teach using a counter in the

calculation. Liao teaches the use of a counter value to keep track of the generations of key regeneration (column 15, line 59-61). It would have been obvious to modify Schwenk in view of O'Shea to include a counter value, as taught by Liao, because it would be more efficient to keep track of how many key regenerations have occurred (column 15, lines 59-61).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to CORDELIA KANE whose telephone number is (571)272-7771. The examiner can normally be reached on Monday - Thursday 8:00 - 5:00 EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/C. K./
Examiner, Art Unit 2132

/Benjamin E Lanier/
Primary Examiner, Art Unit 2132